Abstract of the Disclosure

The present invention gives robustness for the denial-of-service to the authentication protocol itself, loads no additional public key computation, and is applicable to any authentication protocol in which the client authenticates the server by sending the client's random number encrypted under the public key of the server. The method for defeating a denial-of-service attack for use in a communication system in which the client sends a ciphertext of a random number chosen by the client encrypted under a public key of the server to authenticate the server, includes the steps of: (a) the server's generating a random number r_B in response to a service request from the client and sending the random number to the client; (b) the server's receiving the ciphertext which the client produced by using the random number r_B from the client and a random number r_A of the client; (c) the server's recovering a random number r_B from the ciphertext received from the client and comparing the recovered random number with the random number sent to the client; and (d) if the random numbers match at the step (c), providing the service, and, otherwise, denying the service.